MATEC Web of Conferences **76**, 02037 (2016) DOI: 10.1051/matecconf/20167602037
CSCC 2016

RFID reader immunity test against electrostatic discharge

Martin Pospisilik[1,a], Zdenek Korytak[1], Peter Janku[1] and Rui Miguel Soares Silva[2]

[1]*Faculty of Applied Informatics, Tomas Bata University in Zlin, Nad Stranemi 4511, 76005 Zlin, Czech Republic*
[2]*Laboratório Ubi-NET, Campus do Instituto Politécnico de Beja, Apartado 6155, 7800-295, Beja, Portugal*

Abstract. This paper provides a description of an immunity test against the electrostatic discharge according to the standard EN 61000-4-2 that was applied to an RFID reader. The RFID reader was primarily developed for access systems, employing the on-board recognition of the RFID tags. The results obtained by the test are described hereby as well as the discussion on the security of this solution. The results of this experiment are beneficial for the developers of RFID devices, as these devices are endangered by the electrostatic discharge brought by their users. The hereby described results also shown a security hole in a simple access system based on the RFID technology. Details can be found in the paper.

1 Introduction

The issues on electrostatic discharges have been solved since the beginning of the 19th century when several paper mills had faced the accidents caused by ignition of the paper dust by spark discharges. Even earlier, the effects on spark discharges on gunpowder have also been known [3]. However, the problems of the electrostatic discharges have been comprehensively tackled since the first field-effect semiconductors begun to be employed. Nowadays the electrostatic discharge (ESD) protection is one of the most important issues at the electronic devices' development as the current semiconductors exhibit high sensitivity to the energy released during the discharge.

At present, testing of devices on the immunity to electrostatic discharges falls within the tests performed within the framework of electromagnetic compatibility (EMC) testing. In European Union the conditions and criteria of testing on the ESD immunity are described by the standard EN 61000-4-2. This standard prescribes the criteria that must be fulfilled when the tested device is in operation as well.

2 Local electrostatic discharge

The local electrostatic discharge occurs between two surfaces provided there is a significant difference between their charges that are determined by the number of accumulated electrons. Lightning is probably the most dramatic effect of ESD, but in practice, even in much smaller discharges high powers are dissipated, which can result in unpleasant consequences. Although the typical energy released at one ESD reaches the order of mJ, due to very short discharge times (nanoseconds) the levels of voltage and current are destructive to most of the semiconductor devices. According to [2] the charge on the surface of a human body can reach up to 15 kV when walking or rubbing on clothing. A typical current waveform when ESD occurs is depicted in figure 1.

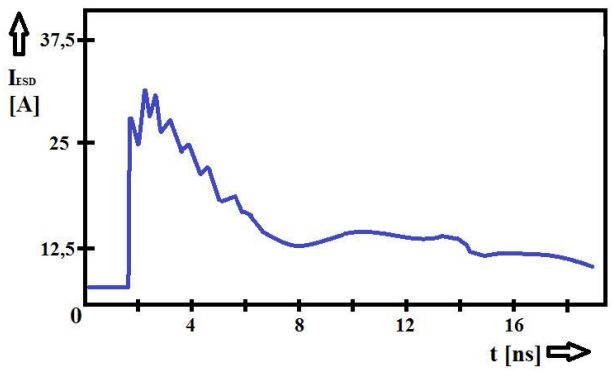

Figure 1. Typical current waveform during the electrostatic discharge [2].

The electrostatic discharge may occur both naturally and artificially as a result of operation of the device. With the participation of the human element, the following cases can occur:

- Electrostatic discharge between two entities provided one of them is charged and the other one is grounded, typically when a technician touches a part of the circuit with some instruments.
- Electrostatic discharge between the charged human body and the grounded electrical circuit, typically when an operator touches the control elements.

[a] Corresponding author: pospisilik@fai.utb.cz

In order to prevent the above mentioned situations, a set of test that must be underwent by the tested devices, is prescribed by the standard EN 61000-4-2.

3 Standardization

As mentioned above, testing of any electronic device's immunity against ESD falls among the issues on electromagnetic susceptibility. The generic standard EN 61000-6-1 defines functional criteria according to which the performance of the tested device can be objectified. The description of these criteria is provided in the table below.

Table 1. Functional criteria according to EN 61000-6-1.

Criterion	Description
A	No influence of the external energy to the operation of the device has been observed.
B	The device operates according to the specification, but some of its characteristics are partially affected by the interferences. The interferences do not change data in the memory of the device nor its operating state. Once the interference disappeared, the proper operation of the whole device is restored without the operator's intervention.
C	The interference interrupted the proper operation of the device or its part and the operator's intervention is needed to recover the device to its normal operation.
(D)	The interference caused damage to the device or its part.

The ESD immunity test is defined by the standard EN 61000-4-2. By means of this standard, the voltage levels, pulse waveforms and the configuration of the experiment are prescribed as well as the steps of the experiment. As the source of energy ESD simulators are used. Generally, three types of ESD tests can be applied, as described in the subchapters below.

3.1. Direct discharge through air gap

The principle of the direct discharge through an air gap is depicted in Fig. 2. The tested device (EuT) is placed on a wooden table the surface of which is covered by a grounded metal plate. On the floor of the testing area the grounded reference metal plate must be placed as well.

The discharge is generated by means of the ESD simulator, which is in the figure denoted by the letter "S". The block diagram of the simulator is depicted in Fig. 3. The main part of the simulator is the accumulating capacitor C_0 the capacity of which must be 150 pF. The capacitor is charged from the high voltage source. The output voltage of this source must be adjustable at least from 2 to 15 kV. The charging resistor R_0 limits the charging current as well as the output current of the simulator once the capacitor is discharged. Its resistance must be as high as 50 to 100 MΩ. According to the Czech version of EN 61000-4-2 the discharge resistor R must embody the resistance of 330 Ω.

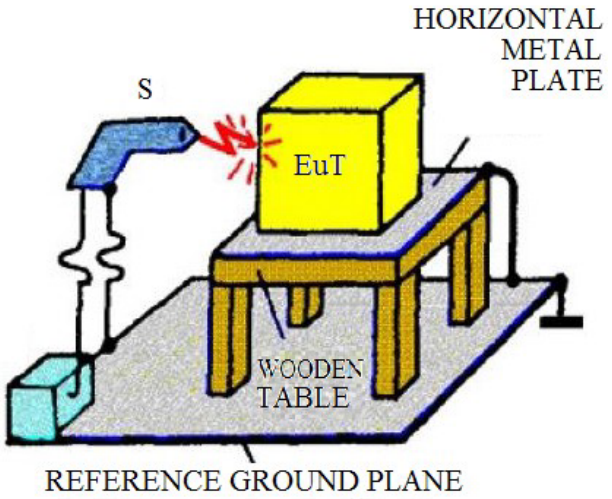

Figure 2. Direct discharge through the air gap – experiment configuration [1].

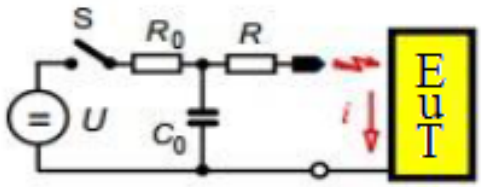

Figure 3. Block diagram of the ESD simulator generating the discharge through the air gap [1].

When processing the experiment, the operator moves the tip of the simulator toward to the tested device. Once the dielectric strength of the air gap is overcome, the energy stored in the capacitor C_0 is dissipated to the tested device by means of the discharge.

However, this type of experiments is not preferred due to its poor repeatability. When repeated, the waveform of the dissipation current can differ according to the air humidity, speed of the simulator tip's movement, air pressure and other variables.

3.2 Discharge through the contact

This experiment eliminates the disadvantages of the test by means of the discharge through the air gap. The ESD simulator touches the tested device by means of a conductive contact. This configuration allows better control over the amount of the dissipated energy and the time course of its handover.

The configuration of the experiment is depicted in Fig. 4. The placement of the tested device is the same as in the previous case as well as the configuration of the whole experiment, but the operator touches the device (EuT) by the conductive tip of the simulator and triggers the discharge by the "trigger" contact.

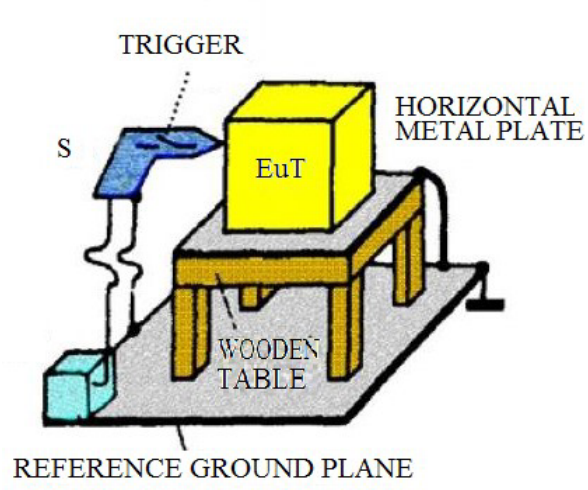

Figure 4. Discharge through the contact – experiment configuration [1].

The block diagram of the simulator is depicted in Fig. 5. The principle of its operation is the same as described in the subchapter above. Also the values of the devices R_0, C_0 and R are the same, but there is a switch denoted as "K" that triggers the discharge to the tested device (EuT).

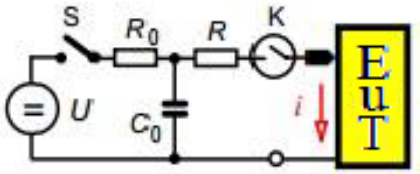

Figure 5. Block diagram of the ESD simulator generating the discharge through the direct contact [1].

The typical discharge current time course at this kind of experiment is depicted in Fig. 6. The levels of the currents I_{30} and I_{60}, referring to the time period of 30 and 60 ns after the discharge was triggered, are dependent on the voltage on the capacitor C_0. The theoretical levels are enlisted in Table 2.

Table 2. Theoretical current pulse parameters.

Charge voltage [V]	I_{max} [A]	I_{30} [A]	I_{60} [A]
2	7.5	4	2
4	15	8	4
6	22.5	12	6
8	30	16	8

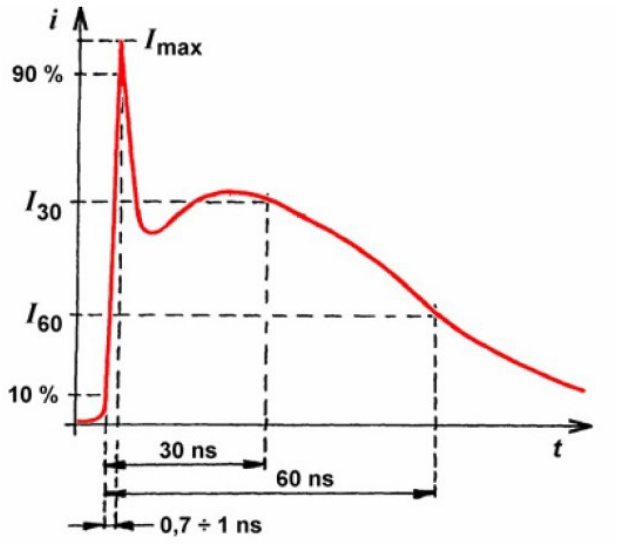

Figure 6. Typical time course of the discharge current at the direct discharge experiment [1].

3.3 Indirect discharge

This experiment simulates the situation in which the device is not directly hit by the electrostatic discharge, but some other objects in its neighbourhood are. The configuration of this experiment is depicted in Fig. 7.

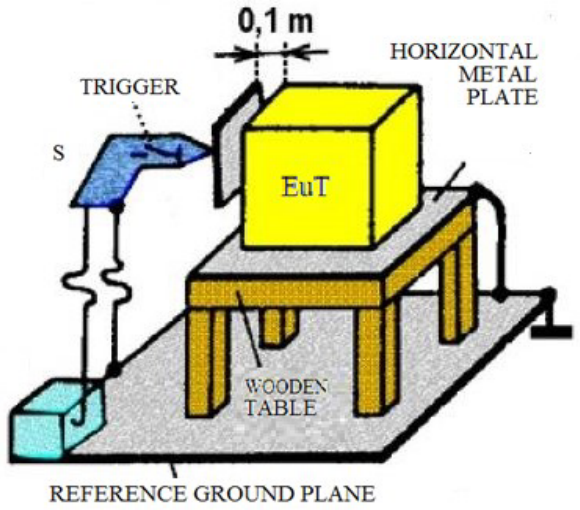

Figure 7. Indirect discharge – experiment configuration [1].

In this experiment, the horizontal coupling plane is placed 0.1 m far from the tested device. This plane is driven by the direct contact discharge. The experiment is repeated ten times for each side of the device. The construction of the simulator is as depicted in Fig. 5.

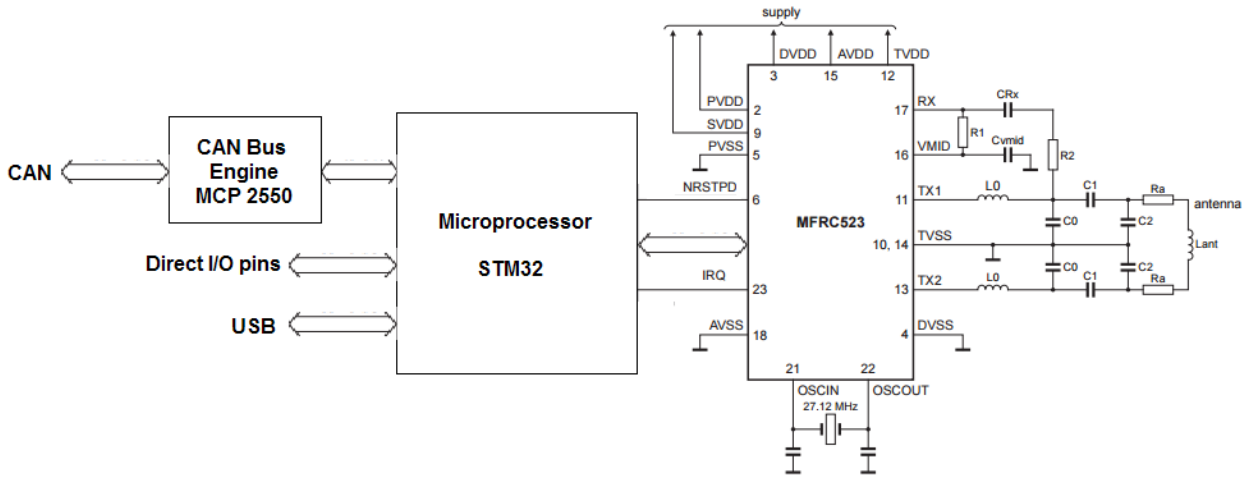

Figure 8. Simplified schematic diagram of the RFID reader.

3.4 Selection of testing points

The type of the experiment as well as the points of the tested device that are exposed to the ESD are selected according to the expected method of the device's use. Usually, the following critical parts of the device are tested:

- AC/DC mains terminals,
- Signal terminals,
- Control elements,
- Cover of the device.

4 Tested RFID reader

This chapter describes the RFID reader that was a subject to the ESD testing. The block diagram of the reader is depicted in Fig. 8.

The heart of the reader is the microprocessor from the family STM32F that has a direct connection to the RFID reader chip MFRC523. This chip provides a complete RFID interface for reading of tags implemented in access cards. The detailed description of this chip can be found in [4]. The data interface of the reader is assured by several ports:

- CAN Bus based on the engine MCP 2550,
- USB implemented directly in the microprocessor,
- Direct parallel port connected to the microprocessor's I/O pins.

To simplify the test, the following algorithm has been implemented to the reader. The microcontroller periodically requests the RFID chip to check whether there is a readable tag. Once the tag is enclosed to the reader's antenna, its unique number is read and when it is recognized, a set of logical bits is sent to the direct parallel port of the reader. This implementation cam be for example used in simple authentication systems where the actuator (door opening etc.) is driven directly by the RFIR reader. Moreover, there is a LED connected to one of the output pins to indicate the logical level at the appropriate output.

5 Experiment description

The experiment was held according to the requirements specified by the standards EN 61000-6-1 and EN 61000-4-2. The configuration of the experiment was held according to the figures 2, 4 and 7. To process the experiment, the test generator Haeffely ONYX 16 was employed. It embodies the following features:

- Replaceable tip for both type of discharges – with and without the air gap,
- Adjustable voltage from 1 to 16 kV,
- Plus or minus polarity.

The tested RFID reader was supplied from a laboratory power source. The configuration of the experiment is depicted in Fig. 9.

Figure 9. The RFID reader and the ESD generator ONYX 16 [5].

The test voltages were increased from the basic level of 1 kV up to the levels prescribed by the above mentioned standards:

- ± 4 kV for a contact discharge,
- ± 8 kV for a discharge through the air gap.

The ESD was applied to the following parts of the RFID reader:

- Input and output pins,
- Status LED,

- RFID antenna.

6 The results

The results achieved at the test are enlisted in the Table 3. The functional criteria have been evaluated according to Table 1.

To fulfil all the requirements of the standard EN 61000-4-2, the worst achieved result should not be worse than B. As obvious from the Table 3, in one case this requirement has not been met. However, it must be considered, that the tested device was operated without the proper cover and the contact discharge was targeted directly to the receiver's antenna. This problem can be solved by enclosing the reader into a suitable cover.

After processing of the test the device has been checked for its proper operation and it has been found that no permanent damage occurred.

Unfortunately, the test shown another problem that is not covered by the requirements of the standard. When the device was influenced by the ESD, several logical 1 states occurred at the direct parallel bus. That means that there exists a real risk if the RFID reader is used directly to drive the actuators (for example the door lock), consisting in the fact that the attacker would bypass the authentication by giving the ESD shock to the RFID reader. On the other hand, this risk can be eliminated by using the modulated and/or encoded output peripherals as the CAN bus or USB. In this case, the RFID reader only gives the information on reading of the tag to another device that manages the actuators driving and the existence of accidental pulses on the communication bus cause no harm to the safety of the authentication system.

7 Conclusions

In this paper a description of the ESD immunity test on a typical construction of the RFID reader is provided. The results of the test indicate, that if the RFID reader is intended to be used in a safety critical application, for example as a controller of the door lock, the phenomenon of the electrostatic discharge cannot be omitted, as the ESD can be generated deliberately as a kind of attack to the system. In this test a possibility of generating a false positive signals at the output of the reader was confirmed. Therefore we recommend not to use the RFID reader directly to recognize the tags, but to process the information on the tags in the neighbourhood of the reader's antenna by the remote device.

Acknowledgements

This work was supported by the Ministry of Education, Youth and Sports of the Czech Republic within The National Sustainability Programme Project No. LO1303 (MSMT-7778/2014) and also by The European Regional Development Fund under the project CEBIA-Tech No. CZ.1.05/2.1.00/03.0089.

References

1. J. Svacina, *Electromagnetic compatibility [Elektromagneticka kompatibilita]* (VUT Brno, 2001, ISBN 80-21418737)
2. P. Horsky, *Electrostatic discharge and testing of its influence on integrated circuits [Elektrostatický výboj a testování jeho vlivu na elektromagnetické pole]* (Online, 2014, URL: http://design.georgius.cz/sites/infocube/eem/horsky_eem081.pdf)
3. I. Poole, *ESD Protection* (Online, 2014, URL: https://radio-electronics.com)
4. MFRC523 (datasheet, 2016)
5. Z. Korytak, *Testing the Electromagnetic Susceptibility of Electrical Appliances* (Diploma thesis, Supervisor: M. Pospisilik)

Table 3. Results of the test.

Point of ESD application	Charge voltage	Discharge type	Polarity	Result
I/O pins	4 kV	Contact	(+)	B
			(-)	B
LED (output state indicator)	4 kV	Contact	(+)	B
			(-)	B
RFID antenna	4 kV	Contact	(+)	C
			(-)	B
The whole reader through a vertical coupling plane	4 kV	Vertical coupling plane	(+)	A
			(-)	B
I/O pins	8 kV	Air gap	(+)	B
			(-)	B
LED (output state indicator)	8 kV	Air gap	(+)	B
			(-)	B
RFID antenna	8 kV	Air gap	(+)	B
			(-)	B